REMARKS

The present Amendment amends claims 14, 17 and 18, and leaves claims 15 and 16 unchanged. Therefore, the present application has pending claims 14-18.

Interview Summary

Applicants thank the Examiner for granting the interview conducted on May 8, 2008. In the interview, arguments were presented to overcome the cited references, particularly Beebe et al. ("Beebe"). The Examiner indicated that Applicants' arguments regarding claims 14 and 18 appeared to overcome the Beebe reference. However, the Examiner indicated that further search and consideration would be required. In this response, Applicants have reiterated the arguments made during the interview.

35 U.S.C. §112 Rejections

Claim 17 stands rejected under 35 U.S.C. §112, second paragraph as allegedly failing to particularly point out and distinctly claim the subject matter of the invention. This rejection is traversed for the following reasons. Applicants submit that claim 17, as now more clearly recited, is in compliance with the provisions of 35 U.S.C. §112.

35 U.S.C. §102 Rejections

Claims 14-16 and 18 stand rejected under 35 U.S.C. §102(e) as being anticipated by U. S. Patent No. 6,226,372 to Beebe et al. ("Beebe"). This rejection is traversed for the following reasons. Applicants submit that the features of the present invention as now more clearly recited in claims 14-16 and 18 are not taught or suggested by Beebe whether taken individually or in

combination any of the other references of record. Therefore, Applicants respectfully request the Examiner to reconsider and withdraw this rejection.

Amendments were made to the claims to more clearly describe features of the present invention. Specifically, amendments were made to the claims to more clearly recite that the present invention is directed to a security management method and system as recited, for example, in independent claims 14 and 18.

The present invention, as recited in claim 14, and as similarly recited in claim 18, provides a security management method for supporting security management of a plurality of managed systems executed in an information system, which includes computers connected through a network. The method includes designing security specifications to be applied to the information system by using an information security policy designated by a user. According to the present invention, the information security policy is applied to each of the plurality of managed systems designated by the user. Also according to the present invention, the information security policy is selected from a first database, which includes a correspondence between information security policies and security measures. Furthermore, according to the present invention, each security measure indicates an action to be taken to secure the managed systems. The method also includes auditing a security status of the information system with respect to the information security policy designated by the user, where the security status indicates whether a security measure has been executed. Furthermore, the method includes auditing system information of each of the plurality of managed systems, where the

system information comprises a version of a software program installed in each respective managed system, and a type of apparatus in which each respective managed systems operates. Even further, the method includes changing the security status of each of the managed systems based on a result of auditing the security status and the system information. Also, the method includes auditing the security status of the information system and the system information every time a security setting is changed. The prior art does not disclose all of these features.

The above described features of the present invention, as now more clearly recited in the claims, are not taught or suggested by any of the references of record, particularly Beebe, whether taken individually or in combination with any of the other references of record.

Beebe teaches a tightly integrated cooperative telecommunications firewall and scanner having distributed capabilities. However, there is no teaching or suggestion in Beebe of the security management method and system as recited in claims 14 and 18 of the present invention.

Beebe discloses a system and method for implementing a fully integrated and cooperative telecommunications firewall/scanner that can be deployed either as a standalone device, or over a large-scale distributed client-server architecture. In addition to providing telecommunications firewall and scanner security capabilities, the integrated telecommunications firewall/scanner provides the capability to ensure implementation of a corporate-dictated security structure, and event visibility and report consolidation requirements, across a globally-distributed enterprise, using

policy-based enforcement of a Security Policy. In the most basic configuration, the integrated firewall/scanner performs continuous security access monitoring and control functions, keyword and content monitoring and control functions, and remote access authentication, initiating coordinated vulnerability assessments, as well as automatic synchronous adjustments to the Security Policy in response to the vulnerability assessment results. Additionally, firewall and scanner actions, assessment results, and responses can be consolidated in detailed or summary reports for use by security administrators for trend analysis and security posture decision-making. The same Security Policy is used by both the firewall and the scanner components of the integrated firewall/scanner during both their cooperative and independent operations.

One feature of the present invention, as recited in claim 14, and as similarly recited in claim 18 includes auditing system information of each of the plurality of managed systems, where the system information includes a version of a software program installed in each respective managed system, and a type of apparatus in which each respective managed systems operates. Beebe does not disclose this feature.

As described in column 10, lines 21-25, Beebe discloses where the scanner component 14 continuously executes a scan to detect the type of device (i.e., fax, mode or voice) on each extension. This is not the same as the present invention, where system information of each of the managed systems is audited, and where the system information includes a version of a software program installed in each respective managed system, and a type of

apparatus in which each respective managed systems operates. Accordingly, Beebe is quite different from the present invention.

Another feature of the present invention, as recited in claim 14, and as similarly recited in claim 18, includes changing the security status of each of the managed systems based on a result of auditing the security status and the system information. Beebe does not disclose this feature.

As previously discussed, Beebe does not teach auditing system information in the manner claimed. Therefore, it follows that Beebe does not disclose changing the security status of each of the managed systems based on a result of auditing the security status and the system information. Furthermore, the Examiner relies upon column 9, lines 52-67 to support the assertion that Beebe teaches changing the security status of each of the management system. However, neither the cited text nor any other portion of Beebe, teaches or suggests where the security status of each of the managed systems is changed based on a result of auditing the security status and the system information, as now more clearly recited in the claims.

Yet another feature of the present invention, as recited in claim 14, and as similarly recited in claim 18, includes auditing the security status of the information system and the system information every time a security setting is changed. Beebe does not disclose this feature.

To support the assertion that Beebe teaches auditing the security status every time the security setting is changed, the Examiner cites column 11, lines 12-26. However, neither the cited text nor any other portion of Beebe teaches or suggests auditing the security status of the information

system and the system information every time a security setting is changed, as now more clearly recited in the claims.

Therefore, Beebe fails to teach or suggest "auditing system information of each of the plurality of managed systems, wherein the system information comprises a version of a software program installed in each respective managed system, and a type of apparatus in which each respective managed systems operates" as recited in claims 14 and 18.

Furthermore, Beebe fails to teach or suggest "changing the security status of each of the managed systems based on a result of auditing the security status and the system information" as recited in claims 14 and 18.

Further, Beebe fails to teach or suggest "auditing the security status of the information system and the system information every time a security setting is changed" as recited in claims 14 and 18.

Therefore, Beebe does not teach or suggest the features of the present invention, as recited in claims 14-16 and 18. Accordingly, reconsideration and withdrawal of the 35 U.S.C. §102(e) rejection of claims 14-16 and 18 as being anticipated by Beebe are respectfully requested.

The remaining references of record have been studied. Applicants submit that they do not supply any of the deficiencies noted above with respect to the references used in the rejection of claims 14-16 and 18.

35 U.S.C. §103 Rejections

Claim 17 stands rejected under 35 U.S.C. §103(a) as being unpatentable over Beebe in view of CERT's CC Vendor-Intitiated Bulletins

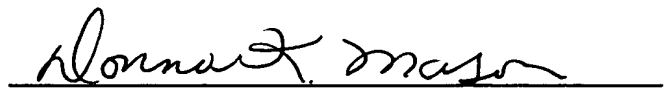
1994-1998. Claim 17 is dependent on claim 14. Therefore, claim 17 is allowable for the same reason previously discussed regarding independent claim 14.

In view of the foregoing amendments and remarks, Applicants submit that claims 14-18 are in condition for allowance. Accordingly, early allowance of claims 14-18 is respectfully requested.

To the extent necessary, the applicants petition for an extension of time under 37 CFR 1.136. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, or credit any overpayment of fees, to the deposit account of MATTINGLY, STANGER, MALUR & BRUNDIDGE, P.C., Deposit Account No. 50-1417 (referencing Attorney Docket No. 566.39530VX1).

Respectfully submitted,

MATTINGLY, STANGER, MALUR & BRUNDIDGE, P.C.



Donna K. Mason
Registration No. 45,962

DKM/cmd
(703) 684-1120